Orders Modulo A Prime

How to make life easier

by M Ahsan Al Mahir
on August 22, 2020

Recap

* Euler and Fermat's Theorem
* Modular Inverses
* Bezout's Identity

Recap

* Euler and Fermat’s Theorem
* Modular Inverses
* Bezout’s Identity

We all know the following theorem, right?

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Where $\phi(n)$ is the number of numbers that are coprime to n and are smaller than n.

We all know the following theorem, right?

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Where $\phi(n)$ is the number of numbers that are coprime to n and are smaller than n.

We can use this theorem in the following way:

$$a^m \equiv a^{m \pmod{\phi(n)}} \pmod{n}$$

So for example, if n $= 12, \phi(12) = 4$ and so:

$$7^{13} \equiv 7^{13 \pmod 4} \equiv 7^{1} \pmod{12}$$

Recap

* Euler and Fermat’s Theorem
* Modular Inverses
* Bezout’s Identity

If a and n are `coprime integers`, then there exists a positive integer $b < n$ such that

$$ab \equiv 1 \pmod{n}$$

If a and n are `coprime integers`, then there exists a positive integer $b < n$ such that

$$ab \equiv 1 \pmod{n}$$

Why do we need inverses?

If a and n are `coprime integers`, then there exists a positive integer $b < n$ such that

$$ab \equiv 1 \pmod{n}$$

Why do we need inverses? We can use them in place of division by a:

$$\frac{1}{a} \equiv b \pmod{n}$$

If a and n are `coprime integers`, then there exists a positive integer $b < n$ such that

$$ab \equiv 1 \pmod{n}$$

Why do we need inverses? We can use them in place of division by a:

$$\frac{1}{a} \equiv b \pmod{n}$$

So adding or multiplying by $\frac{1}{a}$ is just adding or multiplying by b modulo n.

So if there are two integers s, t such that

$$a^s \equiv a^t \pmod{n}$$

then we can say

$$a^{s-t} \equiv 1 \pmod{n}$$

So if there are two integers s, t such that

$$a^s \equiv a^t \pmod{n}$$

then we can say

$$a^{s-t} \equiv 1 \pmod{n}$$

In other words, if a is coprime to n, we can divide congruences modulo n by a.

Note that if $\gcd(a, n) \neq 1$, then it doesn't hold.

Note that if $\gcd(a, n) \neq 1$, then it doesn't hold.

6 can never divide $2a - 1$.

Note that if $\gcd(a, n) \neq 1$, then it doesn't hold.

6 can never divide $2a - 1$.

Just like that $\gcd(n, a)$ must divide 1, because it divides $ab - 1$. And so the gcd has to be 1.

Recap

* Euler and Fermat’s Theorem
* Modular Inverses
* Bezout’s Identity

Another useful identity to remember is for all integer a, b, we will find two integers x, y such that

$$ax + by = \gcd(a, b)$$

Orders

* Why do we care?
* So what is “Order”?
* Important Properties of Order
* Usage in Problems
* Something more fundamental
* Conclusion

Orders

* Why do we care?
* So what is “Order”?
* Important Properties of Order
* Usage in Problems
* Something more fundamental
* Conclusion

Suppose you are told to count the remainder of 10^{561} when divided by 73, how would you do it?

Suppose you are told to count the remainder of 10^{561} when divided by 73, how would you do it?

One trick you learned in Fermat's Little Theorem is to reduce the exponent by $\phi(73)$ which happens to be 72.

Suppose you are told to count the remainder of 10^{561} when divided by 73, how would you do it?

One trick you learned in Fermat's Little Theorem is to reduce the exponent by $\phi(73)$ which happens to be 72.

You can do:

$$\begin{aligned} 10^{72} &\equiv 1 \pmod{73} \\ \text{and, } 561 &\equiv 57 \pmod{72} \\ \text{so, } 10^{561} &\equiv 10^{57} \pmod{73} \end{aligned}$$

Suppose you are told to count the remainder of 10^{561} when divided by 73, how would you do it?

One trick you learned in Fermat's Little Theorem is to reduce the exponent by $\phi(73)$ which happens to be 72.

You can do:

$$\begin{aligned} 10^{72} &\equiv 1 \pmod{73} \\ \text{and, } 561 &\equiv 57 \pmod{72} \\ \text{so, } 10^{561} &\equiv 10^{57} \pmod{73} \end{aligned}$$

But then *again*, you need to count 10^{57} which is near impossible!!

But what if I told you,

$$10^8 \equiv 1 \pmod{73} \quad ?$$

But what if I told you,

$$10^8 \equiv 1 \pmod{73} \quad ?$$

Then your life would become so easy that you could just write

$$10^{561} \equiv 10^{561 \pmod 8} \equiv 10^1 \pmod{73}$$

Orders

* Why do we care?
* So what is “Order”?
* Important Properties of Order
* Usage in Problems
* Something more fundamental
* Conclusion

» Definition

If a and n are coprime integers, then the Order of a modulo n is the smallest integer m such that

$$a^m \equiv 1 \pmod{n}$$

» Definition

If a and n are coprime integers, then the Order of a modulo n is the smallest integer m such that

$$a^{m} \equiv 1 \pmod{n}$$

We write it as

$$\mathrm{Ord}_{n}(a) = m$$

» Definition

If a and n are coprime integers, then the Order of a modulo n is the smallest integer m such that

$$a^m \equiv 1 \pmod{n}$$

We write it as

$$\mathrm{Ord}_n(a) = m$$

In our previous example, since $10^8 \equiv 1 \pmod{73}$, we say

$$\mathrm{Ord}_{73}(10) = 8$$

As more example, below are given the orders of a modulo 11 and 13:

a	mod 11	mod 13
1	1	1
2	10	12
3	5	3
4	5	6
5	5	4
6	10	12

a	mod 11	mod 13
7	10	12
8	10	4
9	5	3
10	2	6
11		12
12		2

Orders

* Why do we care?
* So what is "Order"?
* Important Properties of Order
* Usage in Problems
* Something more fundamental
* Conclusion

An interesting thing you might have noticed in the last slide: *all* of the orders modulo 11 were factors of $10 = \phi(11)$, that are $1, 2, 5, 10$.

An interesting thing you might have noticed in the last slide: all of the orders modulo 11 were factors of $10 = \phi(11)$, that are $1, 2, 5, 10$.

Is this is a coincident or are there more to it?

It turns out it is *a* fundamental property of orders:

It turns out it is a fundamental property of orders:

If m is the order of a modulo n, then $m|\phi(n)$

It turns out it is a fundamental property of orders:

If m is the order of a modulo n, then $m|\phi(n)$

How do you prove it?

It turns out it is a fundamental property of orders:

If m is the order of a modulo n, then $m|\phi(n)$

How do you prove it?

Suppose $m \not| \phi(n)$. So $\phi(n) = mq + r$ for some q and r with $r < m$. (Euclidean division)

It turns out it is a fundamental property of orders:

If m is the order of a modulo n, then $m|\phi(n)$

How do you prove it?

Suppose $m \not| \phi(n)$. So $\phi(n) = mq + r$ for some q and r with $r < m$. (Euclidean division)

Which gives us:

$$a^{\phi(n)} \equiv a^{mq+r} \equiv (a^m)^q \times a^r \equiv a^r \equiv 1 \pmod n$$

But m is the smallest such positive number, so r can't be smaller than m unless $r = 0$!

In fact if $m = \mathrm{Ord}_n(a)$ and for some x,

$$a^x \equiv 1 \pmod{n}$$

then $m | x$

I leave its proof to you!

If for some positive integer s, t we have

$$a^s \equiv a^t \pmod{n}$$

then $s \equiv t \pmod{\mathrm{Ord}_n(a)}$

If for some positive integer s, t we have

$$a^s \equiv a^t \pmod{n}$$

then $s \equiv t \pmod{\mathrm{Ord}_n(a)}$

We solve it by remembering that $a^{s-t} \equiv 1 \pmod{n}$ and that $\mathrm{Ord}_n(a) | s - t$. So,

$$s \equiv t \pmod{\mathrm{Ord}_n(a)}$$

Now we use the idea of orders to prove the following very important theorem:

For an odd prime p, if $a^2 \equiv -1 \pmod{p}$, then

$$4 | p - 1$$

Now we use the idea of orders to prove the following very important theorem:

For an odd prime p, if $a^2 \equiv -1 \pmod{p}$, then

$$4 | p - 1$$

Can you solve it using the properties discussed earlier?

First we sqaure up the congruence to get

$$\left(a^2\right)^2 = a^4 \equiv 1 \pmod{p}$$

First we sqaure up the congruence to get

$$\left(a^2\right)^2 = a^4 \equiv 1 \pmod{p}$$

Then we can say $\mathrm{Ord}_p(a) | 4$ and so $\mathrm{Ord}_p(a)$ is either $1, 2, 4$.

First we sqaure up the congruence to get

$$\left(a^2\right)^2 = a^4 \equiv 1 \pmod{p}$$

Then we can say $\mathrm{Ord}_p(a) | 4$ and so $\mathrm{Ord}_p(a)$ is either $1, 2, 4$.

But $\mathrm{Ord}_p(a)$ can't be $1, 2$. Can you see why?

First we sqaure up the congruence to get

$$\left(a^2\right)^2 = a^4 \equiv 1 \pmod{p}$$

Then we can say $\mathrm{Ord}_p(a) | 4$ and so $\mathrm{Ord}_p(a)$ is either $1, 2, 4$.

But $\mathrm{Ord}_p(a)$ can't be $1, 2$. Can you see why?

Because then a^2 would not be congruent to -1 modulo p.

First we sqaure up the congruence to get

$$(a^2)^2 = a^4 \equiv 1 \pmod p$$

Then we can say $\mathrm{Ord}_p(a)|4$ and so $\mathrm{Ord}_p(a)$ is either $1, 2, 4$.

But $\mathrm{Ord}_p(a)$ can't be $1, 2$. Can you see why?

Because then a^2 would not be congruent to -1 modulo p.

So $\mathrm{Ord}_p(a) = 4$ and that gives us:

$$4|\phi(p) \implies 4|p-1$$

Orders

* Why do we care?
* So what is “Order”?
* Important Properties of Order
* Usage in Problems
* Something more fundamental
* Conclusion

Now that we know what orders *are*, we can try using them in solving problems. Consider the following problem:

Now that we know what orders are, we can try using them in solving problems. Consider the following problem:

Prove that for all integers a, n, we have $n | \phi(a^n - 1)$.

Now that we know what orders are, we can try using them in solving problems. Consider the following problem:

Prove that for all integers a, n, we have $n | \phi(a^n - 1)$.

A lot of number theory problems need to be solved by cleverly finding which modulo to take. This is no exception.

Now that we know what orders are, we can try using them in solving problems. Consider the following problem:

Prove that for all integers a, n, we have $n | \phi(a^n - 1)$.

A lot of number theory problems need to be solved by cleverly finding which modulo to take. This is no exception.

From the idea of orders, we know that $\text{Ord}_m | \phi(m)$ right?

Now that we know what orders are, we can try using them in solving problems. Consider the following problem:

Prove that for all integers a, n, we have $n|\phi(a^n - 1)$.

A lot of number theory problems need to be solved by cleverly finding which modulo to take. This is no exception.

From the idea of orders, we know that $\mathrm{Ord}_m | \phi\,(m)$ right?

So we want to make n as the order of some integer modulo $a^n - 1$.

It turns out a is the integer that we are looking for!! How?

It turns out a is the integer that we are looking for!! How?

We have $a^n \equiv 1 \pmod{a^n - 1}$. Now for any integer $m < n$, we have

$$a^m - 1 < a^n - 1 \implies a^n - 1 \nmid a^m - 1$$

It turns out a is the integer that we are looking for!! How?

We have $a^n \equiv 1 \pmod{a^n - 1}$. Now for any integer $m < n$, we have

$$a^m - 1 < a^n - 1 \implies a^n - 1 \nmid a^m - 1$$

So n is the smallest integer such that $a^n \equiv 1 \pmod{a^n - 1}$, and so

$$\mathrm{Ord}_{a^n-1}(a) = n$$

It turns out a is the integer that we are looking for!! How?

We have $a^n \equiv 1 \pmod{a^n - 1}$. Now for any integer $m < n$, we have

$$a^m - 1 < a^n - 1 \implies a^n - 1 \nmid a^m - 1$$

So n is the smallest integer such that $a^n \equiv 1 \pmod{a^n - 1}$, and so

$$\mathrm{Ord}_{a^n-1}(a) = n$$

And so we have

$$n \mid \phi(a^n - 1)$$

Another problem:

Prove that if p is a prime number, then every prime divisor of $2^p - 1$ is greater than p.

Another problem:

Prove that if p is a prime number, then every prime divisor of $2^p - 1$ is greater than p.

A general tip for these kind of "everything is greater than" problem, it is usually helpful to assume the contrary.

Another problem:

Prove that if p is a prime number, then every prime divisor of $2^p - 1$ is greater than p.

A general tip for these kind of "everything is greater than" problem, it is usually helpful to assume the contrary.

In our case, it will help if instead of `showing that all the prime factors are indeed greater than p`, we assume that there is a prime factor q smaller than p, and show contradiction.

So suppose there exists a prime $q < p$ such that

$$q | 2^p - 1 \implies 2^p \equiv 1 \pmod{q}$$

So suppose there exists a prime $q < p$ such that

$$q | 2^p - 1 \implies 2^p \equiv 1 \pmod{q}$$

We use our knowledge of orders and say that there is an integer $n \leq q - 1$ such that $2^n \equiv 1 \pmod{q}$. Do you see the complication here?

So suppose there exists a prime $q < p$ such that

$$q | 2^p - 1 \implies 2^p \equiv 1 \pmod{q}$$

We use our knowledge of orders and say that there is an integer $n \leq q - 1$ such that $2^n \equiv 1 \pmod{q}$. Do you see the complication here?

Yes! If such n existed, then that would mean $n | p$! But it can't be true, since $n \leq q - 1 < p$, but divides p, a prime number.

So suppose there exists a prime $q < p$ such that

$$q | 2^p - 1 \implies 2^p \equiv 1 \pmod{q}$$

We use our knowledge of orders and say that there is an integer $n \leq q - 1$ such that $2^n \equiv 1 \pmod{q}$. Do you see the complication here?

Yes! If such n existed, then that would mean $n|p$! But it can't be true, since $n \leq q - 1 < p$, but divides p, a prime number.

Wait, but $1|p$, so if $n = 1$, it may happen right?

So suppose there exists a prime $q < p$ such that

$$q | 2^p - 1 \implies 2^p \equiv 1 \pmod{q}$$

We use our knowledge of orders and say that there is an integer $n \leq q - 1$ such that $2^n \equiv 1 \pmod{q}$. Do you see the complication here?

Yes! If such n existed, then that would mean $n | p$! But it can't be true, since $n \leq q - 1 < p$, but divides p, a prime number.

Wait, but $1 | p$, so if $n = 1$, it may happen right?

No! That would mean $q | 2^1 - 1$ which means $q | 1$...

So there can't be a prime $q < p$ that divides $2^p - 1$, and our problem is solved!

Another problem similar to the previous one:

Prove that if p is a prime, then there is a prime greater than p that divides $p^p - 1$.

Another problem similar to the previous one:

Prove that if p is a prime, then there is a prime greater than p that divides $p^p - 1$.

Another prime exponent! Remember what we did just a while ago?

Another problem similar to the previous one:

Prove that if p is a prime, then there is a prime greater than p that divides $p^p - 1$.

Another prime exponent! Remember what we did just a while ago?

We take a prime smaller than q that divides $p^p - 1$. We will have that

$$\mathrm{Ord}_q(p) | p$$

Another problem similar to the previous one:

Prove that if p is a prime, then there is a prime greater than p that divides $p^p - 1$.

Another prime exponent! Remember what we did just a while ago?

We take a prime smaller than q that divides $p^p - 1$. We will have that

$$\mathrm{Ord}_q(p) | p$$

And so $\mathrm{Ord}_q(p) = 1$ and:

$$q | p - 1$$

Do you remember the factorization formula of $a^n - 1$??

$$a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} \cdots + a + 1\right)$$

Do you remember the factorization formula of $a^n - 1$??

$$a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} \cdots + a + 1\right)$$

So,

$$p^p - 1 = (p-1)\left(p^{p-1} + p^{p-2} \cdots + p + 1\right)$$

Do you remember the factorization formula of $a^n - 1$??

$$a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} \cdots + a + 1\right)$$

So,

$$p^p - 1 = (p-1)\left(p^{p-1} + p^{p-2} \cdots + p + 1\right)$$

We have found that if $q < p$, and $q | p^p - 1$, then $q | p - 1$. But what about the $\left(p^{p-1} + p^{p-2} \cdots + p + 1\right)$ part? No smaller prime divides this number.

Do you remember the factorization formula of $a^n - 1$??

$$a^n - 1 = (a-1)\left(a^{n-1} + a^{n-2} \cdots + a + 1\right)$$

So,

$$p^p - 1 = (p-1)\left(p^{p-1} + p^{p-2} \cdots + p + 1\right)$$

We have found that if $q < p$, and $q | p^p - 1$, then $q | p - 1$. But what about the $\left(p^{p-1} + p^{p-2} \cdots + p + 1\right)$ part? No smaller prime divides this number.

So there must be a prime bigger than p that divides this number!!

Now prove that there is a prime factor of $p^p - 1$ of the form $pk + 1$.

Now prove that there is a prime factor of $p^p - 1$ of the form $pk + 1$.

Just before we proved that there is a prime q larger than p that divides $p^p - 1$. Then by order's properties, we need to have

$$\mathrm{Ord}_q(p) = p \text{ or } \mathrm{Ord}_q(p) = 1$$

Now prove that there is a prime factor of $p^p - 1$ of the form $pk + 1$.

Just before we proved that there is a prime q larger than p that divides $p^p - 1$. Then by order's properties, we need to have

$$\mathrm{Ord}_q(p) = p \text{ or } \mathrm{Ord}_q(p) = 1$$

But it won't be 1 !

Now prove that there is a prime factor of $p^p - 1$ of the form $pk + 1$.

Just before we proved that there is a prime q larger than p that divides $p^p - 1$. Then by order's properties, we need to have

$$\mathrm{Ord}_q(p) = p \text{ or } \mathrm{Ord}_q(p) = 1$$

But it won't be 1 ! Because then $q | p - 1$, but q is bigger than p!

Now prove that there is a prime factor of $p^p - 1$ of the form $pk + 1$.

Just before we proved that there is a prime q larger than p that divides $p^p - 1$. Then by order's properties, we need to have

$$\mathrm{Ord}_q(p) = p \text{ or } \mathrm{Ord}_q(p) = 1$$

But it won't be 1 ! Because then $q|p - 1$, but q is bigger than p!

So the order of p modulo q is p, and so $p|\phi(q)$, which means $p|q - 1$.

Now prove that there is a prime factor of $p^p - 1$ of the form $pk + 1$.

Just before we proved that there is a prime q larger than p that divides $p^p - 1$. Then by order's properties, we need to have

$$\mathrm{Ord}_q(p) = p \text{ or } \mathrm{Ord}_q(p) = 1$$

But it won't be 1 ! Because then $q | p - 1$, but q is bigger than p!

So the order of p modulo q is p, and so $p | \phi(q)$, which means $p | q - 1$.

That means $q - 1 = pk \implies q = pk + 1$ for some integer k.

Orders

* Why do we care?
* So what is “Order”?
* Important Properties of Order
* Usage in Problems
* Something more fundamental
* Conclusion

As you have seen, orders are really interesting when the modulo is a prime. And since the order always divide $p - 1$, a natural question comes up:

As you have seen, orders are really interesting when the modulo is a prime. And since the order always divide $p-1$, a natural question comes up:

When is the order equal to $p-1$?

As you have seen, orders are really interesting when the modulo is a prime. And since the order always divide $p-1$, a natural question comes up:

When is the order equal to $p-1$?

We have a special name for such a's for which

$$\mathrm{Ord}_p(a) = p - 1$$

» Primitive Roots

We call an integer a smaller than p a `Primitive Root` modulo p if the order of a modulo p is $p - 1$.

» Primitive Roots

We call an integer a smaller than p a `Primitive Root` modulo p if the order of a modulo p is $p - 1$.

In our very first example, we saw that for 11, the primitive roots mod 11 are

$$2, 6, 7, 8$$

» Primitive Roots

We call an integer a smaller than p a `Primitive Root` modulo p if the order of a modulo p is $p - 1$.

In our very first example, we saw that for 11, the primitive roots mod 11 are

$$2, 6, 7, 8$$

And for 13 the primitive roots mod 13 are

$$2, 6, 7, 11$$

» Primitive Roots

We call an integer a smaller than p a `Primitive Root` modulo p if the order of a modulo p is p -1.

In our very first example, we saw that for 11, the primitive roots mod 11 are

$$2, 6, 7, 8$$

And for 13 the primitive roots mod 13 are

$$2, 6, 7, 11$$

We won't dive too deep into the world of primitive roots, since it is really Huge, we will just see why they are so important!

If g is primitive root modulo p, then the two sets

$$\{g^1, g^2 \dots g^{p-1}\} \text{ and } \{1, 2, 3 \dots p-1\}$$

are equal in modulo p.

If g is primitive root modulo p, then the two sets

$$\{g^1, g^2 \dots g^{p-1}\} \text{ and } \{1, 2, 3 \dots p-1\}$$

are equal in modulo p.

In the case of 11, we can work it out by hand, if we take the primitive root 2 the left set becomes:

g^k	mod 11	g^k	mod 11
2	2	64	9
4	4	128	7
8	8	265	3
16	5	512	6
32	10	1024	1

So if we can find *a* primitive root, we can just keep multiplying it to itself and get the whole set $\{1, 2, \ldots p - 1\}$. Pretty cool huh?

Orders

* Why do we care?
* So what is “Order”?
* Important Properties of Order
* Usage in Problems
* Something more fundamental
* Conclusion

In short, orders are the smallest integer m that gives us $a^m \equiv 1 \pmod{n}$, and they appear everywhere once you start looking for them.

» Further Reading

$a^n \pm 1$ by Yufei Zhao

» Further Reading

$a^n \pm 1$ by Yufei Zhao

Orders Modulo A Prime by Evan Chen

» Further Reading

$a^n \pm 1$ by Yufei Zhao

Orders Modulo A Prime by Evan Chen

Topics in Number Theory: An Olympiad-Oriented Approach by Masum Billal and Amir Hossein Parvardi